UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,034	02/06/2004	Scott E. Hrastar	4682	7739

22474 7590 11/20/2008

CLEMENTS BERNARD MILLER
1901 ROXBOROUGH ROAD
SUITE 300
CHARLOTTE, NC 28211

EXAMINER	
SANTIAGO CORDERO, MARIVELISSE	
ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
11/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/774,034	HRASTAR, SCOTT E.	
	Examiner	Art Unit	
	MARIVELISSE SANTIAGO-CORDERO	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on 9/17/2008 have been fully considered but they are not persuasive.

Applicant argues that Zuk et al.'s (hereinafter "Zuk") MMIDP system does not deal with the wireless network (Remarks: page 8, last paragraph). In response the Examiner respectfully disagrees. Zuk discloses that MMIDP sensors are placed at the gateway points of a wireless network (paragraph [0083]); also shown in Fig. 3, reference 70. Zuk further discloses that it should be understood by one skilled in the art that remote office local area network 50, local area network 60, and DMZ 55 may comprise any electronic device capable of connecting to the Internet or other network operating with common protocols via a wireless network (paragraph [0084]). Therefore, Zuk's MMIDP system does deal with the wireless network.

Applicant argues that Zuk does not teach wireless policy as recited in the claims - wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings, given that Zuk does not see the packets until they reach the wired network; and therefore, it is not possible for Zuk to teach wireless policy since the system taught by Zuk only sees packets after they enter the wired network from the base station 72 (Remarks: page 8, last paragraph). In response, the Examiner respectfully disagrees. At the outset, Zuk discloses that the network security policy defines which traffic to inspect and which attacks the MMIDP sensors should look for (paragraph [0078]). As explained above, Zuk discloses that MMIDP sensors are placed at the gateway points of a wireless network (paragraph

[0083]) and that it should be understood by one skilled in the art that remote office local area network 50, local area network 60, and DMZ 55 may comprise any electronic device capable of connecting to the Internet or other network operating with common protocols via a wireless network (paragraph [0084]); therefore, possible for Zuk to teach wireless policy. Furthermore, Zuk discloses existing network security technologies, which maintain their privacy through the use of security procedures involving authentication and encryption (paragraphs [0005]-[0008]) and choosing an authentication method by comparing the method the client supports against security policy (paragraph [0015]). Therefore, Zuk does disclose wireless policy as recited in the claims, i.e., wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings.

Applicant argues that paragraphs [0005]-[0008] in Zuk are not relevant to wireless policy as claimed by applicants (Remarks: page 9, 1st full paragraph). In response, the Examiner respectfully disagrees. The wireless policy as claimed by applicant comprises a deviation from a set of one or more wireless policy settings comprising, among other, authentication settings. Zuk's paragraphs [0005]-[0008] and [0015] are relevant because they disclose existing network security technologies, which maintain their privacy through the use of security procedures involving authentication and encryption (paragraphs [0005]-[0008]) and choosing an authentication method by comparing the method the client supports against security policy (paragraph [0015]). As explained above, Zuk discloses that MMIDP sensors are placed at the gateway points of a wireless network (paragraph [0083]) and that it should be understood by one skilled in the art that remote office local area network 50, local area network 60, and DMZ 55

may comprise any electronic device capable of connecting to the Internet or other network operating with common protocols via a wireless network (paragraph [0084]); therefore, given such disclosure one of ordinary skill in this art would understand that the techniques (e.g., security policy) applied to the wired networks (Fig. 3, references 50, 55, and 65) would be equally applicable to wireless network.

Applicant argues that Zuk fails to disclose, teach, or suggest wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings (Remarks: page 9, 1st full paragraph). In response, Applicant's arguments are more specific than claims. The claim specifically requires a set of one or more policy settings, not all of the policy settings cumulatively, as argued. As explained above, Zuk discloses wireless policy settings comprising authentication settings (see previous paragraph); and, therefore, meeting the claim.

Applicant argues that Zuk also fails to disclose, teach or suggest wireless statistics and that Applicant's wireless statistics not only include the alarms, but also are used to generate alarms through various wireless-related thresholds (Remarks: page 9, 2nd full paragraph). In response, the Examiner respectfully disagrees. Applicant's arguments are more specific than claims. The features upon which applicant relies (i.e., wireless statistics not only include the alarms, but also are used to generate alarms through various wireless-related thresholds) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In addition, in paragraph [0111], Zuk discloses updating a signature-specific count, e.g., to count how many different hosts were contacted from

the same IP address, during a given time period, and so on (paragraph [0111]), i.e., wireless statistics. If the count is above a pre-determined threshold, then an alarm is generated (paragraph [0111]). Accordingly, Zuk does disclose utilizing wireless statistics in the dynamic operational and security assessments as claimed.

Applicant disagrees with the Examiner that the same techniques in wired intrusion detection systems would apply to wireless (Remarks: page 9, 2nd full paragraph). In response, as explained above, Zuk discloses that MMIDP sensors are placed at the gateway points of a wireless network (paragraph [0083]) and that it should be understood by one skilled in the art that remote office local area network 50, local area network 60, and DMZ 55 may comprise any electronic device capable of connecting to the Internet or other network operating with common protocols via a wireless network (paragraph [0084]); therefore, given such disclosure one of ordinary skill in this art would understand that the techniques applied to the wired networks would be equally applicable to wireless network.

Applicant argues that it is not possible for Zuk to teach the tests since Zuk views packets after they leave the base station (Remarks: page 9, last paragraph). In response, the Examiner respectfully disagrees. Zuk discloses that MMIDP sensors are placed at the gateway points of a wireless network (paragraph [0083]). Zuk also discloses that MMIDP sensors may operate in gateway mode to drop any incoming or outgoing suspicions packets before reaching the network hosts or the outside network (paragraph [0048]); therefore, possible for Zuk to perform these tests.

In response to applicant's argument that the Challener fails to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., stripping

header information off wireless packets for gather statistics and for performing these tests) (Remarks: page 9, last paragraph) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant argues that it is not possible to combine Challener and Zuk since Zuk monitors packets only on a wired portion of the network (i.e., without corresponding wireless header information) and Challener does not teach storing and processing wireless header information (Remarks: page 9, last paragraph). In response the Examiner respectfully disagrees. At the outset, it is noted that the features upon which applicant relies (i.e., storing and processing wireless header information) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In addition, the Examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to combine was found in the references themselves, i.e., for accurately and comprehensively detecting and preventing network security breaches by integrating multiple methods of security detection (Zuk: Abstract; paragraphs [0042], [0044], [0046], [0056]); defining which traffic to inspect and which attacks the sensor should look for (Zuk: paragraph [0054]), and organizing reports that provide access to network statistics (Zuk:

paragraphs [0055], [0082]). In addition, as previously explained, Zuk discloses that MMIDP sensors are placed at the gateway points of a wireless network (paragraph [0083]) and that MMIDP sensors may operate in gateway mode to drop any incoming or outgoing suspicions packets before reaching the network hosts or the outside network (paragraph [0048]). Therefore, it is possible to combine them.

Applicant argues that detecting attacks is not detecting anomalous behavior and that it is not possible for the combination of Challener and Zuk to detect authorized wireless devices which are displaying anomalous behavior because neither teaches gathering wireless statistics (Remarks: page 10, 1st-2nd full paragraphs). In response, the Examiner respectfully disagrees. In paragraph [0111], Zuk discloses updating a signature-specific count, e.g., to count how many different hosts were contacted from the same IP address, during a given time period, and so on (paragraph [0111]), i.e., wireless statistics. If the count is above a pre-determined threshold, then an alarm is generated (paragraph [0111]). Zuk also discloses that intrusion detection systems collects information from a variety of system and network resources to analyze the information for signs of intrusion (i.e., attacks coming from outside the network) and misuse (i.e., attacks originating from inside the network) (paragraph [0025]). Detecting misuse is fairly characterized (and understood by those of ordinary skill in the art) as detecting authorized wireless devices which are displaying anomalous behavior. Accordingly, Zuk does disclose detect authorized wireless devices which are displaying anomalous behavior. Nevertheless, in the last Office Action, references Campbell was used for further support for this limitation.

Moreover, it is noted that claim 1 is directed to an apparatus. It should be emphasized that, in accordance with **MPEP 2114**, while features of an apparatus may be recited either

structurally or functionally, claims directed to an apparatus claims must be distinguished from the prior art in terms of structure rather than function. *In re Danly*, 263 F. 2d 844, 847, 120 USPQ 528, 531 (CCPA 1959). Apparatus claims must be structurally distinguishable from the prior art. I*n Hewlett-Packard Co. v Bausch & Lomb Inc.*, 909 F.2d 1464, 1469, 15 USPQ2d 1525, 1528 (Fed. Cir. 1990), the court held that: "Apparatus claims cover what a device is, not what it does". To emphasize the point further, the court added: "An invention need not operate differently than the prior art to be patentable, but need only be different". The cited references disclose all the structural limitations of the claim; therefore, meeting claim 1.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-12, 15-16, and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener in views of and Zuk et al. (hereinafter "Zuk"; Pub. No.: US 2003/0154399) and Campbell et al. (Patent No.: US 6,893,850).

Regarding claim 1, Challener discloses a system for tracking location of a wireless device, the system comprising:

a system data store (paragraph [0027]; note the server) capable of storing indicators of one or more wireless devices to track (paragraph [0027]);

a set of one or more wireless receivers on one or more wireless sensors (paragraphs [0025]-[0029]; note the workstations, wireless access points, and monitoring stations and that monitoring check the activity of access points sensed; thus, on one or more wireless sensors);

a system processor in communication with the system data store and the one or more wireless sensors (paragraphs [0026]-[0028]), wherein the system processor comprises one or more processing elements programmed or adapted to perform the steps comprising of:

(a) identifying a wireless device for tracking based upon data from the system data store (Fig. 3; paragraph [0027]);

(b) receiving data from a subset of the one or more wireless sensors (paragraphs [0026]-[0029]; note the workstations, monitoring stations, and wireless access point);

(c) storing the received data in the system data store (paragraphs [0027]-[0029]);

(d) calculating the position of the identified wireless device based upon the stored data (paragraphs [0028]-[0029]); and

(e) outputting the calculated position (Fig. 3, last step; note that the stored determined location and identity are retrieved by IT management; thus, outputted).

Challener fails to specifically disclose the system data store capable of storing one or more tracking criteria and identifying based upon a combination of dynamic operational and security assessments derived using data from the system data store, wherein the dynamic operational and security assessments identify the wireless device for tracking responsive to behavior of the wireless device, wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, wherein the policy deviation-based tests

comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings, and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings; and wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments, wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior. Note, however, that Challener discloses monitoring during normal business hours (paragraph [0025]); thus, suggesting tracking criteria.

Nonetheless, in the same field of endeavor, Zuk discloses the system data store capable of storing one or more tracking criteria (paragraph [00081], [0100], [0113]-[0115]) and identifying based upon a combination of dynamic operational and security assessments derived using data from the system data store (Fig. 13; paragraphs [0111], [0113]-[0115]), wherein the dynamic operational and security assessments identify the wireless device for tracking responsive to behavior of the wireless device (paragraphs [0046], [0052], [0111], [0113]-0115]), and wherein the dynamic operational and security assessments comprise wireless signature-based tests (Fig. 13; paragraphs [0029], [0102]-[0103], [0114]; see *Response to Arguments* section above), wireless protocol-based tests (Fig. 13; paragraphs [0029], [0032], [0100], [0113] ; see *Response to Arguments* section above), wireless anomaly-based tests (Fig. 13; paragraphs [0111], [0115] ; see *Response to Arguments* section above), and wireless policy deviation-based tests (Fig. 13; paragraphs [0032], [0054], [0075], [0081], [0117] ; see *Response to Arguments* section above), and wherein the policy deviation-based tests comprise a deviation from a set of one or more

wireless policy settings (paragraphs [0005]-[0008], [0015], [0022]-[0023], and [0054]) comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings (paragraphs [0005]-[0008], [0015] and [0054]; note that when a client starts a session, it first sends a list of authentication method it supports, the firewall then compares these methods against security policy defined by the network administrator, chooses which one to use and authenticates the client; thus, comprising a deviation from a set of one or more of the wireless policy settings claimed, fairly characterized as the claimed authentication settings; see *Response to Arguments* section above), and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings (paragraphs [0005]-[0008], [0015], [0022]-[0023], and [0054]); and wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments (paragraphs [0055], [0082] and [0111]; *Response to Arguments* section above).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to store in the system data store of Challener one or more tracking criteria and identifying based upon a combination of dynamic operational and security assessments derived using data from the system data store, wherein the dynamic operational and security assessments identify the wireless device for tracking responsive to behavior of the wireless device, and wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings; wherein the policy

deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings; and wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments as suggested by Zuk for the advantages of accurately and comprehensively detecting and preventing network security breaches by integrating multiple methods of security detection (Zuk: Abstract; paragraphs [0042], [0044], [0046], [0056]); defining which traffic to inspect and which attacks the sensor should look for (paragraph [0054]), and organizing reports that provide access to network statistics (paragraphs [0055], [0082]).

Challener in combination with Zuk fails to specifically disclose wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior. Note, however, that Zuk discloses these limitations. Zuk discloses that intrusion detection systems collects information from a variety of system and network resources to analyze the information for signs of intrusion (i.e., attacks coming from outside the network) and misuse (i.e., attacks originating from inside the network) (paragraph [0025]). Detecting intrusion is fairly characterized (and understood by those of ordinary skill in the art) as detection of unauthorized devices and detecting misuse is fairly characterized (and understood by those of ordinary skill in the art) as detecting authorized wireless devices which are displaying anomalous behavior.

Nevertheless, in the same field of endeavor, Campbell discloses wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized

wireless devices and authorized wireless devices which are displaying anomalous behavior (col. 2, lines 25-61; col. 4, lines 43-44; col. 10, lines 50-61; col. 13, lines 4-19 and 33-57).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to modify the wireless statistics of Challener in combination with Zuk to enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior as suggested by Campbell for the advantages of providing early indications and warnings of a suspected intrusion or misuse (Campbell: col. 1, lines 8-20).

Regarding claim 2, in the obvious combination, Zuk discloses wherein one or more tracking criteria are of a type selected from the group consisting of time, traffic level, threat level, protocol characteristics, usage characteristics or combinations thereof (paragraphs [0100], [0111], [0114]-0115]). Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to select the one or more tracking criteria from the group consisting of time, traffic level, threat level, protocol characteristics, usage characteristics or combinations thereof as suggested by Zuk for the advantages of accurately, quickly, and comprehensively detecting and preventing network security breaches by integrating multiple methods of security detection (Zuk: Abstract; paragraphs [0042], [0044], [0046], [0056]).

Regarding claim 3, in the obvious combination, Zuk discloses wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of dynamically determining one or more tracking criteria (paragraphs [0100], [0111], [0113]-[0115]). Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to dynamically determine one or more tracking criteria as

suggested by Zuk for the advantages of accurately, quickly, and comprehensively detecting and preventing network security breaches by integrating multiple methods of security detection (Zuk: Abstract; paragraphs [0042], [0044], [0046], [0056]).

Regarding claim 4, in the obvious combination, Challener discloses wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) repeat steps (a) through (e) continuously (paragraph [0025]; note that the steps may be performed periodically as distinguished from continuously; however, it is not excluding it from being continuously performed. Thus, Challener suggests that the steps (a) through (e) can be performed continuously).

Regarding claim 5, in the obvious combination, Challener discloses wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) repeat steps (a) through (e) periodically (paragraph [0025]).

Regarding claim 6, in the obvious combination, Challener discloses wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (g) modifying the period of repetition of step (f) (paragraph [0030]), but fail to specifically disclose based upon one or more tracking criteria. However, Challener does disclose monitoring once an hour or once a day during normal business hours so as to avoid imposing an excessive burden on other uses of the devices; thus suggesting based upon one or more tracking criteria. Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to (g) modifying the period of repetition of step (f) based upon one or more tracking criteria as suggested for the advantages of avoiding imposing an excessive burden on other uses of the devices (Challener: paragraph [0030]).

Regarding claim 7, the limitations are rejected with the same grounds and for the same reasons stated above for claim 2.

Regarding claim 8, in the obvious combination, Challener discloses wherein the programming or adaptation to identify the wireless device includes programming or adaptation to perform the step comprising of selecting the identified wireless device based upon indicators of one or more wireless devices in the system data store (Fig. 3; paragraph [0027]).

Regarding claim 9, in the obvious combination, Challener discloses wherein the one or more processing elements are further programmed or adapted to perform the step comprising of (f) detecting an unauthorized wireless device (Fig. 3; paragraph [0027]) and (g) storing an indicator of the unauthorized wireless device in the system data store (Fig. 3, last step; paragraph [0027]).

Regarding claim 10, in the obvious combination, Challener discloses wherein the identified wireless device is the unauthorized wireless device (Fig. 3; paragraph [0027]).

Regarding claim 11, in the obvious combination, Challener discloses wherein the programming or adaptation to identify the wireless device includes further programming or adaptation to perform the step comprising of retrieving indicators of one or more wireless devices from the system data store (Fig. 3; paragraph [0027]).

Regarding claim 12, in the obvious combination, Challener discloses wherein the programming or adaptation to calculate the position of the identified wireless device includes programming or adaptation to perform the steps comprising of:

(i) sensing the identified wireless device (paragraph [0026]);

(ii) storing RF signal characteristics in the system data store based upon the sensing (Challener: paragraph [0027]); and

(iii) dynamically selecting one or more additional sensors to improve tracking performance (paragraphs [0026]-[0029]).

Regarding claim 15, in the obvious combination, Challener discloses wherein the calculated position is output to a user or to a computer system (Fig. 3; last step; note that the calculated position is retrieved by IT management; thus outputted to a user or to a computer system).

Regarding claim 16, in the obvious combination, Challener discloses wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) storing the calculated position in the system data store (Fig. 3, last step; note the "stored determined location and identity").

Regarding claim 19, Challener discloses a method for tracking location of a wireless device, the method comprising the steps of:

(a) detecting a wireless device (Fig. 3; paragraphs [0026]-[0027]);

(b) adding an indicator associated with the detected wireless device to a list of wireless devices (Fig. 3; paragraphs [0026]-[0027])

(c) selecting a wireless device for tracking based upon the list of wireless devices (Fig. 3; paragraphs [0026]-[0027]);

(d) receiving data from one or more wireless sensors (paragraphs [0025]-[0029]; note the workstations, wireless access points, and monitoring stations)

(e) calculating a position of the selected wireless device based upon the received data (Fig. 3; paragraphs [0026]-[0029])

(f) outputting the calculated position (Fig. 3, last step; note that the stored determined location and identity are retrieved by IT management; thus, outputted;

(g) repeating steps (a) and (b) upon occurrence of an event or at periodic intervals (paragraphs [0025] and [0030]);

(h) repeating steps (c) through (f) upon occurrence of an event or at periodic intervals (paragraphs [0025] and [0030]).

Challener fail to specifically disclose detecting utilizing one or more dynamic operational and security assessments, wherein the one or more dynamic operational and security assessments detect the wireless device responsive to behavior of the wireless device, and wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings; and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings; and wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments, wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior. Note, however, that Challener discloses monitoring during normal business hours (paragraph [0025]); thus, suggesting tracking criteria.

Nonetheless, in the same field of endeavor, Zuk discloses the system data store capable of storing one or more tracking criteria (paragraph [0081], [0100], [0113]-[0115]) and identifying based upon a combination of dynamic operational and security assessments derived using data from the system data store (Fig. 13; paragraphs [0111], [0113]-[0115]), wherein the dynamic operational and security assessments identify the wireless device for tracking responsive to behavior of the wireless device (paragraphs [0046], [0052], [0111], [0113]-0115]), and wherein the dynamic operational and security assessments comprise wireless signature-based tests (Fig. 13; paragraphs [0029], [0102]-[0103], [0114]; see *Response to Arguments* section above), wireless protocol-based tests (Fig. 13; paragraphs [0029], [0032], [0100], [0113] ; see *Response to Arguments* section above), wireless anomaly-based tests (Fig. 13; paragraphs [0111], [0115] ; see *Response to Arguments* section above), and wireless policy deviation-based tests (Fig. 13; paragraphs [0032], [0054], [0075], [0081], [0117] ; see *Response to Arguments* section above), and wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings (paragraphs [0005]-[0008], [0015], [0022]-[0023], and [0054]) comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings (paragraphs [0015] and [0054]; note that when a client starts a session, it first sends a list of authentication method it supports, the firewall then compares these methods against security policy defined by the network administrator, chooses which one to use and authenticates the client; thus, comprising a deviation from a set of one or more of the wireless policy settings claimed, fairly characterized as the claimed authentication settings); and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings (paragraphs [0005]-[0008], [0015], [0022]-[0023], and [0054]); and

wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments (paragraphs [0055], [0082] and [0111]; *Response to Arguments* section above).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to store in the system data store of Challener one or more tracking criteria and identifying based upon a combination of dynamic operational and security assessments derived using data from the system data store, wherein the dynamic operational and security assessments identify the wireless device for tracking responsive to behavior of the wireless device, and wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings; wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings; and wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments as suggested by Zuk for the advantages of accurately and comprehensively detecting and preventing network security breaches by integrating multiple methods of security detection (Zuk: Abstract; paragraphs [0042], [0044], [0046], [0056]); defining which traffic to inspect and which attacks the sensor should look for (paragraph [0054]), and organizing reports that provide access to network statistics (paragraphs [0055], [0082]).

Challener in combination with Zuk fails to specifically disclose wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior. Note, however, that Zuk discloses these limitations. Zuk discloses that intrusion detection systems collects information from a variety of system and network resources to analyze the information for signs of intrusion (i.e., attacks coming from outside the network) and misuse (i.e., attacks originating from inside the network) (paragraph [0025]). Detecting intrusion is fairly characterized (and understood by those of ordinary skill in the art) as detection of unauthorized devices and detecting misuse is fairly characterized (and understood by those of ordinary skill in the art) as detecting authorized wireless devices which are displaying anomalous behavior.

Nevertheless, in the same field of endeavor, Campbell discloses wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior (col. 2, lines 25-61; col. 4, lines 43-44; col. 10, lines 50-61; col. 13, lines 4-19 and 33-57).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to modify the wireless statistics of Challener in combination with Zuk to enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior as suggested by Campbell for the advantages of providing early indications and warnings of a suspected intrusion or misuse (Campbell: col. 1, lines 8-20).

Regarding claim 20, Challener in combination with Zuk disclose one or more computer readable media storing instruction that upon execution by a system processor cause the system processor to perform the method of claim 19 (Challener: Fig. 4; paragraph [0031]; see rationale as previously discussed above for claim 19), and wherein the system processor comprises a distributed processor between one or more wireless sensors and a host system (Zuk: Fig. 3; paragraphs [0028], [0048]).

Regarding claim 21, Challener discloses a system for tracking location of a wireless device, the system comprising:

storing means for storing indicators of one or more wireless devices to track (paragraph [0027]);

one or more wireless sensors for scanning wireless traffic (paragraphs [0025]-[0029])

distributed rogue detection means for receiving scan data (paragraphs [0026]-[0029]), for detecting a wireless device based upon the received scan data (paragraphs [0026]-[0029]) and for storing an indicator of the detected wireless device (Fig. 3; paragraphs [0026]-[0029]); and

position determining means for selecting a wireless device to track from the indicators in the storing means (Fig. 3; paragraphs [0026]-[0029]), receiving scan data from one or more wireless receivers (Fig. 3; paragraphs [0026]-[0029]), estimating the position of the selected wireless device based upon received scan data (Fig. 3; paragraphs [0026]-[0029]) and outputting the estimated position (Fig. 3, last step; note that the stored determined location and identity are retrieved by IT management; thus, outputted).

Challener fail to specifically disclose wherein the distributed rogue detection means is distributed between the one or more wireless sensors and a host system; the storing means for

storing one or more tracking criteria and the rogue detection means for detecting based upon one or more dynamic operational and security assessments operable to detect the wireless device based on behavior, wherein the assessments are performed on the received scan data;

wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, and wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings; and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings; and wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments, wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior.

Note, however, that Challener discloses monitoring during normal business hours (paragraph [0025]); thus, suggesting tracking criteria.

Nonetheless, in the same field of endeavor, Zuk discloses wherein the distributed rogue detection means is distributed between the one or more wireless sensors and a host system (Fig. 3; paragraphs [0028], [0048]); the storing means for storing one or more tracking criteria paragraph ([0081], [0100], [0113]-[0115]) and detecting a wireless device based upon one or more dynamic operational and security assessments operable to detect the wireless device based on behavior (Fig. 13; paragraphs [0046], [0052], [0111], [0113]-[0115]), wherein the assessments are performed on the received scan data (Fig. 13; paragraphs [0046], [0052], [0111],

[0113]-[0115]), wherein the dynamic operational and security assessments comprise wireless signature-based tests (Fig. 13; paragraphs [0029], [0102]-[0103], [0114]; see *Response to Arguments* section above), wireless protocol-based tests (Fig. 13; paragraphs [0029], [0032], [0100], [0113] ; see *Response to Arguments* section above), wireless anomaly-based tests (Fig. 13; paragraphs [0111], [0115] ; see *Response to Arguments* section above), and wireless policy deviation-based tests (Fig. 13; paragraphs [0032], [0054], [0075], [0081], [0117] ; see *Response to Arguments* section above), and wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings (paragraphs [0005]-[0008], [0015], [0022]-[0023], and [0054]) comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings (paragraphs [0015] and [0054]; note that when a client starts a session, it first sends a list of authentication method it supports, the firewall then compares these methods against security policy defined by the network administrator, chooses which one to use and authenticates the client; thus, comprising a deviation from a set of one or more of the wireless policy settings claimed, fairly characterized as the claimed authentication settings); and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings (paragraphs [0005]-[0008], [0015], [0022]-[0023], and [0054]); and wherein the received scan data is utilized to update wireless statistics used in the dynamic operational and security assessments (paragraphs [0055], [0082] and [0111]; *Response to Arguments* section above).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to distributed the rogue detection means of Challener between the one or more wireless sensors and a host system, to store in the storing means of Challener one or more

tracking criteria and detecting based upon one or more dynamic operational and security assessments operable to detect the wireless device based on behavior, wherein the assessments are performed on the received scan data, wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings, and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings; and wherein the received scan data is utilized to update wireless statistics used in the dynamic operational and security assessments as suggested by Zuk for the advantages of providing network based intrusion detection (Zuk: Fig. 3; paragraphs [0028], [0048]), accurately and comprehensively detecting and preventing network security breaches by integrating multiple methods of security detection (Zuk: Abstract; paragraphs [0042], [0044], [0046], [0056]); defining which traffic to inspect and which attacks the sensor should look for (paragraph [0054]), and organizing reports that provide access to network statistics (paragraphs [0055], [0082]).

Challener in combination with Zuk fails to specifically disclose wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior. Note, however, that Zuk discloses these limitations. Zuk discloses that intrusion detection systems collects information from a variety of system and network resources to analyze the information for signs of intrusion (i.e., attacks coming from outside the network) and misuse

(i.e., attacks originating from inside the network) (paragraph [0025]). Detecting intrusion is fairly characterized (and understood by those of ordinary skill in the art) as detection of unauthorized devices and detecting misuse is fairly characterized (and understood by those of ordinary skill in the art) as detecting authorized wireless devices which are displaying anomalous behavior.

Nevertheless, in the same field of endeavor, Campbell discloses wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior (col. 2, lines 25-61; col. 4, lines 43-44; col. 10, lines 50-61; col. 13, lines 4-19 and 33-57).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to modify the wireless statistics of Challener in combination with Zuk to enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior as suggested by Campbell for the advantages of providing early indications and warnings of a suspected intrusion or misuse (Campbell: col. 1, lines 8-20).

4. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener in combination with Zuk and Campbell, as applied to claim 1 above, and further in view of Won et al. (hereinafter "Won"; Patent No.: US 6,754,488).

Regarding claim 13, Challener in combination with Zuk disclose the method of claim 1 (see above), but fail to specifically disclose wherein the programming or adaptation to output the calculated position includes programming or adaptation to perform the steps comprising of formatting the calculated position according to one or more output preferences. Note, however,

that at the time of invention by application, output information was notoriously well known in the art to be formatted in order to meet/satisfy the needs/requirements of the receiver.

Nonetheless, in the same field of endeavor, Won discloses wherein the programming or adaptation to output the calculated position includes programming or adaptation to perform the steps comprising of formatting the calculated position according to one or more output preferences (col. 5, lines 23-26; col. 6, lines 36-39; note that visual or audible notification is outputted; thus, the output position is inherently formatted).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to format the calculated position of Challener in combination with Zuk according to one or more output preferences as suggested by Won for the advantages of properly outputting the information and/or meeting the requirements of a receiver and is user-friendlier.

Regarding claim 14, in the obvious combination, Won discloses wherein the calculated position for output is formatted as an e-mail, a web page, a facsimile, a graphic, an XML page, an SNMP message, a page, or combinations thereof (col. 5, lines 23-26; col. 6, lines 36-39). Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to format the calculated position of Challener in combination with Zuk as an e-mail, a web page, a facsimile, a graphic, an XML page, an SNMP message, a page, or combinations thereof as suggested by Won for the advantages of distributing the information in widely available applications that are user-friendly and easily adoptable to the users.

5. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener and Zuk and Campbell as applied to claim 1 above, and further in view of Ammon et al. (hereinafter "Ammon"; cited in IDS).

Regarding claim 17, Challener in combination with Zuk disclose the system of claim 1 (see above), but fails to specifically disclose wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) removing an indicator of a wireless device from the system data store.

However, in the same field of endeavor, Ammon discloses wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) removing an indicator of a wireless device from the system data store (paragraphs [0106]-[0111]; note the active flag).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to remove the indicator of the wireless device from the system data store as suggested by Ammon for the advantages of keeping the most-up-to date information and avoiding filling the data store with duplicate, redundant, and/or unnecessary information.

Regarding claim 18, in the obvious combination, Ammon discloses wherein indicator removal is based upon manual deletion, time deletion, or a change in device security status from unauthorized to authorized (paragraphs [0106]-[0111]; note the active flag).

Therefore, it would have been obvious to one of ordinary skill in this art at the time of invention by applicant to base the indicator removal upon manual deletion, time deletion, or a change in device security status from unauthorized to authorized as suggested by Ammon for the advantages of keeping the most-up-to date information and avoiding filling the data store with duplicate, redundant, and/or unnecessary information.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARIVELISSE SANTIAGO-CORDERO whose telephone number is (571)272-7839. The examiner can normally be reached on Monday through Friday from 8:00am to 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vincent P. Harper can be reached on (571) 272-7605. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VINCENT P. HARPER/
Supervisory Patent Examiner, Art Unit 2617

/MARIVELISSE SANTIAGO-CORDERO/
Examiner, Art Unit 2617